

Desain dan Analisis Pembangkit Bilangan Acak Arnold's Cat map Dengan Inisialisasi Bilangan Logistik

¹⁾ Dimas Akbar Pratama, ²⁾ Alz Danny Wowor,

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo, Salatiga 50714, Indonesia
E-mail: ¹⁾672014151@student.uksw.edu, ²⁾alzdanny.wowor@uksw.edu

Abstract

This study aims to find new methods in strengthening random number generator methods which are then used as keys to cryptography. Random number generator used is Arnold's Cat map chaos, Henon map chaos, and Logistics. All methods are then tested to find the right method to be used as a key to cryptography. Arnold's method of Cat Map with Initialization of logistic numbers as keys that will be added to the plaintext then the results of the addition are added with the following keys so that the encryption made later will get a ciphertext that is difficult to guess.

Keyword : cryptography, Chaos, Arnold Cat Map, Logistic Map, Random Numbers Generator

Abstrak

Penelitian ini bertujuan untuk mencari metode baru dalam memperkuat metode pembangkit bilangan acak yang kemudian dijadikan sebagai kunci pada kriptografi. Pembangkit bilangan acak yang digunakan adalah *Arnold's Cat map chaos*, *Henon map chaos*, dan Logistik. Semua metode itu kemudian diuji untuk mencari manakah metode yang tepat untuk digunakan sebagai kunci pada kriptografi. Metode *Arnold's Cat Map* dengan Inisialisasi bilangan logistik sebagai kunci yang akan ditambahkan dengan *plaintext* kemudian hasil dari penjumlahan tersebut ditambahkan dengan kunci - kunci selanjutnya sehingga enkripsi yang dibuat nanti akan mendapatkan ciphertexts yang sulit di tebak.

Kata Kunci : kriptografi, *Chaos*, *Arnold Cat Map*, *Logistic Map*, Pembangkit Bilangan Acak

¹ Mahasiswa Program studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

² Staff pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga